#4

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ３月３１日

出 願 番 号
Application Number: 特願２０００－０９８８１８

出 願 人
Applicant (s): インターナショナル・ビジネス・マシーンズ・コーポレーション

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ９月１８日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３０７４２４３

【書類名】　特許願

【整理番号】　JP9000086

【あて先】　特許庁長官　殿

【国際特許分類】　H04Q　7/38

H04M　1/66

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　鈴木　慎一郎

【特許出願人】

【識別番号】　390009531

【住所又は居所】　アメリカ合衆国１０５０４、ニューヨーク州アーモンク（番地なし）

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレイション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【選任した代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【手数料の表示】

【予納台帳番号】　024154

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9706050

【包括委任状番号】　9704733

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】通信端末装置によるネットワークへの接続方法および装置

【特許請求の範囲】

【請求項１】識別情報およびパスワードを格納した不揮発性メモリを備え、該識別情報および該パスワードが照合されてネットワークへの通信が許可される通信端末装置から該ネットワークに通信する方法であって、

（ａ）通信の開始時に前記不揮発性メモリに格納した識別情報およびパスワードを前記ネットワークに送信するステップと、

（ｂ）前記ステップ（ａ）で送信したパスワードとは異なるパスワードを前記通信の開始後に生成するステップと、

（ｃ）前記生成したパスワードを前記不揮発性メモリに格納するステップと、

（ｄ）前記生成したパスワードを前記ステップ（ａ）で開始した通信が終了する前に前記ネットワークに送信するステップと

を有する方法。

【請求項２】前記ステップ（ｄ）における生成したパスワードの送信を前記ステップ（ａ）で開始した通信の終了時に実施する請求項１記載の方法。

【請求項３】識別情報およびパスワードを格納した不揮発性メモリを備え、該識別情報および該パスワードが照合されてネットワークへの通信が許可される通信端末装置から、前記識別情報および前記パスワードを格納した記憶装置を備えるネットワークに通信する方法であって、

（ａ）通信の開始時に前記不揮発性メモリに格納した識別情報およびパスワードを受信するステップと、

（ｂ）前記受信した識別情報およびパスワードと前記記憶装置に格納した識別情報およびパスワードとを比較するステップと、

（ｃ）前記ステップ（ｂ）の結果に応答して前記通信端末装置の通信を許可するステップと、

（ｄ）前記ステップ（ａ）で受信したパスワードとは異なるパスワードを前記ステップ（ｃ）で許可された通信が終了する前に受信するステップと、

（ｅ）前記ステップ（ｄ）で受信したパスワードを前記記憶装置に格納するス

テップと
を有する方法。
【請求項４】さらに、前記ステップ（ｄ）で受信したパスワードが前記ステップ（ａ）で通信開始時に受信したパスワードと一致している場合に前記通信端末装置の通信を停止するステップを有する請求項３記載の接続方法。
【請求項５】前記ステップ（ｄ）が前記ステップ（ｃ）で許可された通信の終了時にパスワードを受信する請求項３または請求項４記載の方法。
【請求項６】識別情報およびパスワードを格納した不揮発性メモリを備え、該識別情報および該パスワードが照合されてネットワークへの通信が許可される通信端末装置から前記識別情報および前記パスワードを格納した記憶装置を備えるネットワークに通信する方法であって、
（ａ）通信の開始時に前記不揮発性メモリに格納した識別情報およびパスワードを前記ネットワークに送信するステップと、
（ｂ）前記ステップ（ａ）で送信された識別情報およびパスワードと前記記憶装置に格納した識別情報およびパスワードとを比較するステップと、
（ｃ）前記ステップ（ｂ）の結果に応答して前記通信端末装置の通信を許可するステップと、
（ｄ）前記ステップ（ａ）で送信したパスワードとは異なるパスワードを前記通信の開始後に生成するステップと、
（ｅ）前記生成したパスワードを前記不揮発性メモリに格納するステップと、
（ｆ）前記生成したパスワードを前記ステップ（ｃ）で許可された通信が終了する前に前記ネットワークに送信するステップと
（ｇ）前記ステップ（ｆ）で送信されたパスワードを前記記憶装置に格納するステップと
を有する方法。
【請求項７】識別情報およびパスワードを格納した第１の不揮発性メモリを備え該識別情報および該パスワードが照合されてネットワークへの通信が許可される第１の通信端末装置および、第２の不揮発性メモリを備え該識別情報および該パスワードが照合されてネットワークへの通信が許可される第２の通信端末装置に

よりネットワークに通信する方法であって、

（ａ）前記第１の不揮発性メモリに格納した識別情報およびパスワードを前記第２の不揮発性メモリに格納するステップと、

（ｂ）前記第１の通信端末装置の使用を禁止するステップと、

（ｃ）通信の開始時に前記第２の不揮発性メモリに格納した識別情報およびパスワードを前記ネットワークに送信するステップと、

（ｄ）前記ステップ（ｃ）で送信したパスワードとは異なるパスワードを前記通信の開始後に生成するステップと、

（ｅ）前記生成したパスワードを前記第２の不揮発性メモリに格納するステップと、

（ｆ）前記生成したパスワードを前記ステップ（ｃ）で開始した通信が終了する前に前記ネットワークに送信するステップと

を有する方法。

【請求項８】識別情報およびパスワードを格納した第１の不揮発性メモリを備え該識別情報および該パスワードが照合されてネットワークへの通信が許可される第１の通信端末装置および、第２の不揮発性メモリを備え識別情報およびパスワードが照合されてネットワークへの通信が許可される第２の通信端末装置から、前記識別情報および前記パスワードを格納した記憶装置を備えるネットワークに通信する方法であって、

（ａ）前記第１の不揮発性メモリに格納した識別情報およびパスワードを前記第２の不揮発性メモリに格納するステップと、

（ｂ）前記第１の通信端末装置の使用を禁止するステップと、

（ｃ）通信の開始時に前記第２の不揮発性メモリに格納した前記識別情報および前記パスワードを前記ネットワークに送信するステップと、

（ｄ）前記ステップ（ｃ）で送信された識別情報およびパスワードと前記記憶装置に格納した識別情報およびパスワードとを比較するステップと、

（ｅ）前記ステップ（ｄ）の結果に応答して前記通信端末装置の通信を許可するステップと、

（ｆ）前記ステップ（ｃ）で送信したパスワードとは異なるパスワードを前記

通信の開始後に生成するステップと、

（ｇ）前記生成したパスワードを前記第２の不揮発性メモリに格納するステップと、

（ｈ）前記生成したパスワードを前記ステップ（ｅ）で許可された通信が終了する前に前記ネットワークに送信するステップと

（ｉ）前記ステップ（ｈ）で送信されたパスワードを前記記憶装置に格納するステップと

を有する方法。

【請求項９】前記異なるパスワードがランダムに生成されたパスワードである請求項１ないし８記載の方法。

【請求項１０】識別情報およびパスワードが照合されてネットワークへの通信が許可される通信端末装置であって、

前記識別情報および前記パスワードを格納できる不揮発性メモリと、

通信の開始時に送信したパスワードとは異なるパスワードを生成する手段と、

通信の開始時に前記不揮発性メモリに格納された前記識別情報および前記パスワードを前記ネットワークに送信し、前記生成されたパスワードを前記開始した通信が終了する前に前記ネットワークに送信し、かつ前記不揮発性メモリに格納する手段と

を有する通信端末装置。

【請求項１１】前記パスワードを変更する手段が、ランダムなパスワードを生成する手段である請求項１０記載の通信端末装置。

【請求項１２】前記通信端末装置がさらに前記不揮発性メモリに格納した前記識別情報および前記パスワードを外部に送信しまたは外部から受信するためのポートを備えている請求項１０または請求項１１記載の通信端末装置。

【請求項１３】前記通信端末装置がさらに前記不揮発性メモリに格納した前記識別情報および前記パスワードを格納できる取り外し可能な記憶媒体を装着することができる請求項１０ないし請求項１２のいずれかに記載の通信端末装置。

【請求項１４】識別情報およびパスワードを照合して通信端末装置の通信を許可するネットワーク装置であって、

前記通信端末装置の識別情報およびこれに対応するパスワードを格納した記憶装置と、

通信の開始時に前記通信端末装置から前記識別情報および前記パスワードを受信して、前記記憶装置に格納した前記識別情報および前記パスワードと照合しその結果に応じて前記通信端末装置の通信を許可し、前記開始した通信が終了する前に前記パスワードとは異なるパスワードを前記通信端末装置から受信し前記記憶装置に格納する制御装置と

を有するネットワーク装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は識別情報およびパスワードの照合を条件にしてネットワークへの接続が許可される通信端末装置に関し、より詳細には盗用した識別情報およびパスワードを用いたコピー通信端末装置が不正に利用されている状態を容易に検出してその継続使用を排除する技術に関する。

【０００２】

【従来の技術】携帯電話機は、個人が自由に持ち歩いて利用できるという利便性の故に今日まで急速に普及してきている。携帯電話機には、契約時に通信事業者から機器固有の識別番号と電話番号が割り当てられ内部のメモリに格納される。通話開始時には相手先の電話番号と共に自分の電話番号および識別情報が基地局に送られ、あらかじめ基地局側に登録されている契約者情報と照合された後に相手先に接続され、同時に課金のための時間計算が行われる。もし識別情報および電話番号が他人に盗まれて他の携帯電話機に設定されて使用されてしまうと、課金計算は当該識別情報に基づいて行われるため正規の電話機の所有者は損失を被る。特に、携帯電話機は電波で電話番号および識別情報を送信するので盗用されやすく、たとえ暗号化して送信したとしても解読されて悪用される可能性がでてくる。

【０００３】

したがって、一般に携帯電話機の識別番号は盗用されないように工夫されており、かつ、ユーザは一契約で一つの識別番号とこれに対応する電話番号を備える

携帯電話機を１台だけ保有できるようになっている。特開平８－３４０５７９号公報には、他人の携帯電話機の盗用を防止する技術が開示されている。従来の携帯電話機では、加入者番号、移動局番号、認証および秘匿のキーを含む識別情報がスクランブルコードによってスクランブルされ、そのスクランブルされた識別情報が、ＣＰＵを含んだ制御部の不揮発性ＲＡＭに記憶され、そのスクランブルコードの初期値がその制御部のＲＯＭに記憶されるとともに、その制御部にそのスクランブルコードを発生するアルゴリズムが設けられていた。さらに、そのスクランブルコードの初期値が製品毎に共通であったために、制御部の記憶内容やアルゴリズムを別の携帯電話機の制御部にコピーして、実質的に他人の携帯電話機を盗用することが容易であった。よって、同公報に記載された発明ではスクランブル・コードの初期値を携帯電話機ごとに異なる値で設定し、識別情報をスクランブルしてＥＥＰＲＯＭに書き込み、発呼時にデスクランブルして送信する。

【０００４】

特開平６－２９１８３５号公報には、携帯電話が置き忘れや盗難などにより所有者以外の者の手に渡った場合の無断使用を防止する発明が開示されている。この発明では、電話番号を登録する場合、暗証番号コードが記憶された番号登録装置に携帯電話機を接続する。そして、入力キーにより暗証番号コードを入力する。入力された暗証番号コードが暗証番号コードメモリ内のコードと一致した場合にのみ接続端子を介して携帯電話機の電話番号メモリに電話番号が登録される。登録した電話番号を利用する場合は、携帯電話機の選択キーにより登録されている電話番号の選択コードを入力する。携帯電話機からの送信は登録した電話番号からしかできないため、無断使用の防止が図れる。

【０００５】

特開平４－３１００２６号公報には、通信装置の個別識別番号が故意に読み出されても不当に使用されることを防止する技術が開示されている。この発明では、個別識別番号を所定の手順によりデータ変換して誤り訂正符号とともに記憶し、個別識別番号が不当に使用されることを防止する。さらに、読み出し時、そのデータの誤り訂正をなすとともに個別識別番号に変換し、更に誤り訂正を行った場合はその訂正したデータを記憶手段に記憶させるようにしてデータ破壊を防止

している。

【０００６】

特開平１１－１４６０５７号公報には、移動電話の盗用を防止するためにパスワードを入力しないで個人識別ができるシステムが記載されている。この発明はパスワードを利用して携帯電話機の盗難や紛失による不正使用を防止する技術において、パスワードを覚え入力しなければならない不便さに着目し、音声、呼吸時の二酸化炭素濃度、指紋などのように操作者の身体的特徴を識別子にして他人の不正使用による通話料金の負担を防止している。

【０００７】

一方携帯電話機はたとえ契約者が同一であったとしても、機器固有の識別番号、電話番号等の課金に関する情報が同一の場合、すなわち一契約の場合は１台の電話機しか使用することができないようになっている。この点で、たとえば業務用とプライベート用とで電話機自体を使い分けたい場合には二つの契約を締結しなければならないという不便さがあった。また、通信端末装置として携帯電話機以外に通信機能が備わったＰＤＡやポータブルＰＣなどを利用したい場合にも、別々の契約を締結する必要があった。これを解決する技術として特開平１０－１４５５２３号公報には、端末識別番号が記憶されたカードを利用する技術や、通信ポートを利用して端末識別番号を送受することにより、一契約に対して１台の携帯端末装置を付与するという条件を維持しながら、同一契約者が複数の通信端末装置を利用できる技術が開示されている。

【０００８】

【発明が解決しようとする課題】このように携帯電話機自体が盗難にあったり、識別情報だけが盗用されて他の携帯電話機に設定されることによる不正な使用から携帯電話機の真の所有者を保護する技術が存在している。携帯電話機が盗難や紛失で正規の所有者の手元から離れた場合は、それに気づいた時点で電話会社に連絡して利用を停止すれば損失を最小に押さえることができる。しかし、携帯電話機の所有者に気付かれないように識別番号が盗まれて他の電話機に設定されコピー電話機が製作されてしまうと、通常月単位で送られてくる料金請求書を受け取ってコピー電話機の存在に気付くまでの不正利用による損害は甚大になる可

能性がある。特に、複数のコピー電話機が製作されるとその不正使用による使用料金の損害は一層深刻になる。

【０００９】

前述の従来技術では、たとえスクランブル・コードの初期値を電話機ごとに設定したとしてもそれが盗用されないという保証があるものではなく、またスクランブルするロジックも解析されてしまう可能性がある。また、パスワードの入力を要求する場合でもそのパスワードが盗用されないという保証はなく、その更新・管理および入力も煩雑である。

【００１０】

さらに、一の契約に対して選択的に複数の携帯電話機または通信端末の利用を可能にすることは、それだけ不正にコピー電話機が製作される可能性が高まることを意味しており、従来の方法では十分対処できていなかった。

【００１１】

したがって本発明の目的は、識別情報およびパスワードの識別結果により通信が許可される携帯電話機等の通信端末装置において、パスワードが盗用され他の通信端末装置に設定されてコピー端末として使用されたときに、その状態を容易に認識できる技術を提供することにある。さらに本発明の目的は、他人により不正に製作されたコピー端末の利用を有効に防止しつつ、一契約に対して複数の通信端末装置を選択的に利用できるようにする技術を提供することにある。

【００１２】

【課題を解決するための手段】

本発明の第１の態様は識別情報およびパスワードを格納した不揮発性メモリを備え、該識別情報および該パスワードが照合されてネットワークへの通信が許可される通信端末装置に向けらる。識別情報およびパスワードは英数字、記号等の電子情報として生成できるいかなる符号であってもよい。本態様では通信の開始時にネットワークに送信したパスワードとは異なる新しいパスワードを、一旦開始した通信が終了する以前に生成する。新しいパスワードは毎回の通信の間に生成されるため、ユーザが随時パスワードを変更する場合に比べてパスワードが盗用される確率は低くなる。生成されたパスワードは不揮発性メモリに格納される

のでユーザが記憶し通信のたびにキーを操作して入力する必要がない。新しいパスワードは通信が終了する前にネットワークに送信される。好適には通信の終了時点で通信終了コードと一緒に送信する。したがって、通信端末装置およびネットワークの双方が通信の終了時点で当該通信中に生成した新たなパスワードを保有し、ネットワークは次回の通信開始時にこの新たなパスワードを照合して通信の許可をすることができる。

【００１３】

パスワードは通信のたびに変更されるので、一旦はパスワードだけを盗用してコピー端末を製作したとしても正規の利用者に知られない状態で継続的に使用していくことはできない。すなわち、正規の利用者が正規の通信端末装置を保有して利用している限りパスワードは当該正規の利用者により通信のたびに変更されるので、盗用者は毎回新しいパスワードを盗用しない限りコピー端末の利用ができない。盗用者が正規の利用者と同様に通信のたびにパスワードを変更しながら利用すれば、正規の通信端末装置を利用する際には、ネットワークが認識しているその時点で有効なパスワードでアクセスすることができなくなるので通信は停止され、正規の契約者はパスワードが盗用されていることに気付くことができる。通信端末装置は、無線式または有線式のいづれであってもよく、またポータブル式でも固定式でもよい。

【００１４】

本発明の第２の態様は、通信事業者のネットワークに向けられ、通信端末装置の識別情報およびパスワードを通信の開始時に受信してネットワークの記憶装置に登録されている情報と比較し通信を許可する。さらに当該通信が終了する前に通信開始時に受信したパスワードとは異なるパスワードを受信し記憶装置に格納する。これにより、新しいパスワードを通信端末装置およびネットワークの記憶装置の双方が保有し、次回の通信開始時に通信端末装置から送られた識別番号および新しいパスワードが記憶装置に格納された情報と比較される。

【００１５】

本発明の第３の態様は、第１と第２の２台の通信端末装置からネットワークに通信する場合の通信端末装置に向けられる。一契約のもとでは一台の通信端末装

置しか利用できないが、本発明の態様では、利用できる通信端末装置を選択的に変更してもコピー端末の利用を防止できる。第１の通信端末装置および第２の通信端末装置は、相互に不揮発性メモリに記憶された情報を交換できる周知の機能を備える。その機能は相互の通信ポートに直接ケーブルを接続しても、またネットワークを介して実現してもよい。さらに、不揮発性の記憶媒体に一旦一方の不揮発性メモリの内容を転送し、他の通信端末装置の不揮発性メモリに書き込んでもよい。

【００１６】

第１の通信端末装置の第１の不揮発性メモリに格納した識別情報およびパスワードは第２の通信端末装置の第２の不揮発性メモリに転送・格納される。さらに、第１の通信端末装置は使用禁止にされ、一契約で１台の利用という条件が担保される。第２の不揮発性メモリに転送されたパスワードはその時点でネットワークも保有している有効なパスワードであり、以後第２の通信端末装置は、第１の態様で説明したのと同様の方法で、ネットワークに通信をすることができる。本発明の他の態様は、上記各態様を実現できる通信端末装置およびネットワーク装置に向けられる。

【００１７】

【発明の実施の形態】

図１に本発明の実施の形態を説明するための携帯電話ネットワークの概略図を示す。電話接続事業者が提供する携帯電話ネットワーク２５は、無線の送受信および信号処理を行う基地局１５および１７、携帯電話機が接続される基地局の選定、電話接続制御、課金計算などを行う制御装置１９、契約者情報テーブルを含む記憶装置２１、他の通信ネットワーク２７に接続するための交換機２３を含む。携帯電話機１１から発信した場合は、基地局１５を通じてネットワーク２５に接続され、制御装置１９の制御のもとに基地局１７を通じて他の携帯電話機１３に接続される。または、交換機２３を通じて他の通信ネットワーク２７に接続される。

【００１８】

図２は本発明を適用した携帯電話機１００の概略ブロック図である。アンテナ

１０１は、基地局１５、１７との間で電波の送受信を行う。アンテナ１０１には無線送受信部１０２が接続されている。無線送受信部１０２は音声データと通信データの相互変換および通信データの変調・復調処理を行うとともに、音声データと制御データを分別する。無線送受信部１０２には音声処理部１０３が接続されており音声データを相互に送受信する。音声処理部１０３は音声データと音声信号の相互変換を行う符号・復号器を含む。音声処理部１０３には携帯電話機１００と操作者との音声によるインターフェースの役割を果たすマイク１０５およびスピーカ１０７が接続されている。

【００１９】

制御部１０９はＣＰＵを主体とする構成になっており、携帯電話機１００の動作全体を制御する。制御部１０９には通信インターフェース１１１が接続されている。通信インターフェースはＲＳ２３２Ｃのシリアル・インターフェース・コネクタを含み、電話機と外部とのデータ通信に使用される。また、制御部１０９は無線送受信部１０２および音声処理部１０３に接続されており、無線送受信部１０２との間で制御データを送受信するとともに、これらの動作を制御する。

【００２０】

制御部１０９には、さらにＲＯＭ１１３、ＲＡＭ１１５、不揮発性メモリ１１７が接続されている。ＲＯＭ１１３には、制御部１１３のＣＰＵを動作させるために必要な動作プログラムが格納されており、携帯電話機１００の電源（図示せず。）が喪失しても内容は維持される。ＲＡＭ１１５は、ＣＰＵがデータ処理をする際にデータを一時的に格納するために利用され、携帯電話機の電源が喪失すればその内容は消失する。

【００２１】

不揮発性メモリ１１７は、好適にはフラッシュ・メモリであって電気的に書き込みができるとともに、電源が喪失しても内容を維持することができる。不揮発性メモリ１１７には、電話機を購入する際に販売店で書き込んだ電話機固有の識別番号、電話番号、およびパスワードの初期値が記憶されている。さらに、電話機を購入したユーザが登録した電話番号、電話機の各種設定データ等が記憶されている。不揮発性メモリ１１７に格納した情報は通信インターフェース１１１を

経由して外部と送受信することができる。制御部１０９にはキー操作検出部１１９を経由してキー操作部１２１が接続され、さらに表示制御部１２３を経由してディスプレイ１２５が接続されている。

【００２２】

キー操作部１２１は、ユーザが電話機を操作するための情報を入力するために使用される。キー操作検出部１１９は、操作されたキーに対応したキー・コードを生成し制御部１０９に送る。表示制御回路１２３は、制御部から出力された電話機の動作状態、相手の電話番号等を表す信号を受け取りディスプレイ１２５を制御して内容を表示させる。

【００２３】

つぎに、図２に示した携帯電話機１００の一般的な動作を説明する。電話機を購入した時点では、前述のようにＲＯＭ１１３に動作プログラムが格納されている。また、不揮発性メモリ１１７には、通信インターフェース１１１を経由して設定データの初期値、識別番号、自己の電話番号が書き込まれている。所有者は電話機を購入した後、特定の相手の電話番号や自己にとって操作しやすい状態を示す設定データをキー操作部１２１を操作して不揮発性メモリ１１７に書き込む。さらに携帯電話機１００は、着脱可能な記憶媒体（図示せず）を備えることができる。この記憶媒体に不揮発性メモリ１１７に格納した情報を書き込んだ後に取り外し、他の携帯電話機に装着して、当該他の携帯電話機の不揮発性メモリに情報を転送できるようにすることができる。

【００２４】

いま図２に示した構成を備える携帯電話機２台の間で基地局を経由して通信する場合に、呼び出し側の電話機を図１の携帯電話機１１とし、呼び出される電話機を携帯電話機１３として説明する。電話機１１から電話機１３を呼び出す場合は、まず電話機１１のキー操作部１２１から電話機１３の電話番号を直接入力するか、不揮発性メモリ１１７に格納されている登録電話番号をキー操作部１２１を操作して、ＲＡＭ１１５に読み出す。さらにキー操作部１２１の呼び出しボタンを押して制御部１０９に呼び出し動作を開始させる。制御部１０９は、不揮発性メモリ１１７に記憶されている識別番号および自己の電話番号（電話機１１の

電話番号）をＲＡＭ１１５に呼び出して、電話機１３の電話番号および通信開始コードとともに無線送受信部１０２に送り、搬送波を変調した後アンテナ１０１から変調された呼び出し用の通信データとして基地局に送信する。

【００２５】

基地局には、識別番号、自己の電話番号、住所、氏名等の電話機およびその所有者を特定する情報を含んだ契約者情報テーブルが記憶装置２１に設けられている。電話機１１から呼び出し用の通信データを受け取った基地局１５は、復調および信号処理を行った後に制御装置１９にデータを送る。制御装置１９は、識別番号および送信者の電話番号を契約者情報テーブルの登録データと照合し、適切に登録されている電話機からの呼び出しであると判断した場合に、電話機１３の電話番号に呼び出し信号を転送する。

【００２６】

基地局からアンテナ１０１で呼び出し用の通信データを受け取った電話機１３は、無線送受信部１０２で復調して制御部１０９に送る。制御部１０９は自己の電話が呼び出されていることを判断すると、音声処理部に呼び出し信号を送り、スピーカ１０７から呼び出し音を発生させる。電話機１３の所有者は呼び出し音に応答してキー操作部１２１を操作し制御部１０９に命令を与える。命令を与えられた制御部１０９は無線送受信部１０２および音声処理部１０３を制御して、マイク１０５およびスピーカ１０７を通話をできるようにする。マイク１０５から入力された音声信号は音声処理部１０３で符号化されて音声データに変換される。音声データは無線送受信部１０２に送られ、通信データに変換されて変調され、アンテナ１０１から基地局１７を経由して電話機１１に送られる。

【００２７】

受信者が通話を開始すると制御信号が基地局１７に送られて制御装置１９により課金計算が開始され、送信者の契約者情報テーブルに課金情報が記録される。一方電話機１１は、基地局１５から音声および制御に関する通信データを受信する。アンテナ１０１で受信した変調された通信データは無線送受信部１０２で復調され、制御データは制御部１０９に送られ音声データは音声処理部１０３に送られる。

【００２８】

つぎに、図２に示した携帯電話機１００に本発明を適用した場合の実施形態を図５のフローチャートに従って説明する。本発明を適用するに当たり、ＲＯＭ１１３には図３に示すように、電話機の製造者により動作プログラム１５１およびパスワード変更プログラム１５３が書き込まれている。不揮発性メモリ１１７には図４に示すように、電話機の販売会社によりシステム領域に識別番号、パスワード、および自己の電話番号が書き込まれている。また、ユーザ領域には所有者が入力した電話番号、設定データ等が書き込まれている。パスワードは電話機の販売時点では初期値が格納されており、後に詳しく説明するように、本発明を実行していく課程では通信終了のたびに更新されていく。ネットワーク２５の記憶装置には、図６に示すような契約者情報テーブルが格納されている。

【００２９】

契約者情報テーブルは、契約者ごとに識別番号、電話番号、パスワード、課金情報などが格納されている。パスワードは当初初期値が格納されており、以降で説明するように本発明を実施していく課程で通信ごとに更新されていく。

【００３０】

以後の説明では、すでに説明した電話機１００の一般的な動作に関する部分は割愛または簡略化する。ブロック２０１ではキー操作部１２１を操作して相手の電話番号をＲＡＭ１１５に読み出す。このときブロック２０３において動作プログラム１５１は、識別番号、自己の電話番号とともにパスワードを不揮発性メモリ１１７から読み出してＲＡＭ１１５に格納させる。ＲＡＭ１１５に格納されたこれらのデータは通信開始コードとともに無線送受信部１０２を経由して呼び出し用の通信データとしてネットワーク２５の基地局１５に送られる。ネットワーク２５の記憶装置２１は図６に示す契約者情報テーブル３００を含む。ブロック２０５では、呼び出し用の通信データを受け取った制御装置１９が、識別番号および電話番号に基づいて契約者情報テーブル３００から対応するパスワードを読み出す。

【００３１】

なお、自己の電話番号は必ずしも携帯電話１１から送らなくても識別番号に基

づいて契約者情報テーブルから検索することもできる。ブロック２０７では、電話機１１から送られたパスワードと契約者情報テーブルから読み取られたパスワードとを識別番号を参照しながら照合しブロック２０９で一致・不一致を判断する。ブロック２０９でパスワードが一致していれば、ブロック２１１に移行して制御装置１９は通信を開始させ課金のための通話時間の計算を開始する。ブロック２１３で通信が終了するとユーザはブロック２１５で携帯電話機のキー操作部１２１にある通信終了ボタンを押す。つぎにブロック２１７では、携帯電話機１１の通信終了ボタンが押されたことに応答してパスワード変更プログラム１５３に制御部１０９の制御が移る。パスワード変更プログラム１５３は、この時点で不揮発性メモリ１１７に記憶されているパスワード（古いパスワードという。）とは異なる新しいパスワードを生成し、不揮発性メモリに格納されている古いパスワードに上書きするためのプログラムである。この新しいパスワードは次回の通信のときに使用される次回パスワードとしての意義を有する。

【００３２】

パスワード変更プログラムは古いパスワードと異なるパスワードを生成するものであれば、いかなるプログラムであってもよい。たとえば、古いパスワードと所定の定数との間で演算を行って生成するものでもよいが、好適にはランダムなパスワードを生成するものとすることができる。ランダムなパスワードを生成する手段を備えることにより、たとえ、パスワードの更新ロジックが盗用されたとしても、正規の契約者に発見されないでコピー電話機を使用し続けることは困難になる。なお、ランダムなパスワードはソフトウエアで生成する場合に限定されるものでなく、ハードウエアで生成してもよい。

【００３３】

ブロック２１７で新しいパスワードが生成されると制御部１０９の制御は動作プログラム１５１に移行し、ブロック２１９で次回パスワードと通信終了コードが基地局１５に送られる。ここで、次回パスワードを通信終了時に更新し、ネットワークに送信したが、本発明の趣旨においては通信開始時のパスワードと異なるパスワードを当該通信が終了するまでの間に生成し送信すればよい。

【００３４】

ブロック２２１で通信終了コードを受信した制御装置１９は、課金のための時間計算を終了し、図６に示す契約者情報テーブルのパスワード（古いパスワード）を、通信終了時に電話機１１から送られてきた新しいパスワードで書き換える。電話機１１ではブロック２２３で、不揮発性メモリ１１７内のパスワード格納領域に古いパスワードに対して新しいパスワードを上書きする。ブロック２２１および２２３を実行した時点で電話機１１の不揮発性メモリ１１７および契約者情報テーブル３００はともに同一の新しいパスワード（次回パスワード）を格納していることになる。

【００３５】

電話機の識別番号およびパスワードなどが盗用されてコピー電話機が製作され不正に使用されたときに、本発明の実施の形態では正規の契約者がこれを容易に発見できることが、図５のブロック２０９から分岐したブロック２３１以降の説明で明らかになる。ブロック２０９で携帯電話機１１から送られてきたパスワードと契約者情報テーブル３００のパスワードが同一識別番号に関して一致していないことは、ブロック２２１およびブロック２２３において説明したように、この識別番号および電話番号に関して前回の通信終了時に更新された新しいパスワードを双方が保有していなければならないという前提に反する。

【００３６】

すなわち、不揮発性メモリ１１７および契約者情報テーブル３００への技術的な書き込みエラーを除けば、今回電話機１１から送られてきたパスワードは、前回通信終了時に更新されたパスワードとは異なるものであることを意味する。もし、前回更新されたパスワードが盗用されて識別番号および電話番号とともにコピー電話機に設定され不正に使用されたとすれば、その通信が終了した時点で契約者情報テーブルには更新されたパスワードが格納される。その後正規の利用者が電話機１１から発信しようとすれば不揮発性メモリ１１７に格納されたパスワードは契約者情報テーブルに格納されたものとは異っており、制御装置１９はそれが正規の利用者からの発信であったとしてもブロック２３１で通信を停止する。

【００３７】

さらに制御装置１９はブロック２３３で当該識別番号の携帯電話機の利用を一切禁止する。よって、盗用したパスワードを設定したコピー電話機も以後利用できなくなる。制御装置１９はブロック２３５において、発信してきた携帯電話機にパスワードの盗用による不正使用があったために通信できないことを通知する。この通知により、正規の携帯電話機の保有者はそのパスワードが盗用されたことを知り、通信事業者に手続をしてパスワードおよび識別番号の初期化を行い電話機の利用を再開することができる。

【００３８】

また、パスワードを盗用したコピー電話機が通信終了時にパスワードを更新しないで古いパスワードをネットワークに送ることも予想される。しかし、この場合は制御装置１９が通信終了時に送られたパスワードと通信開始時のパスワードが同一の場合は通信停止にすることで対処できる。また、通信停止にしない場合には正規の契約者が古いパスワードで通信すると通信終了時にパスワードが変更されてしまうので、それ以降盗用者は電話機を利用できなくなる。

【００３９】

本発明の他の実施形態として、一の契約のもとに複数の携帯電話機またはＰＤＡ、ノート型ＰＣなどの通信機能付き通信端末装置を利用させるシステムを説明する。従来技術の項でも説明したように、一の契約のもとでは一台の通信端末装置しか利用できない。いま図７においてユーザが図２および図５に基づいて説明した携帯電話機１００を契約して識別番号、電話番号およびパスワードが付与されているとする。同一ユーザが携帯電話機１００と同一の通信機能を装備したポータブルＰＣ３５０を利用する場合に本発明の実施の形態では、ポータブルＰＣ用に新たに契約を締結する必要がない。

【００４０】

携帯電話機１００からポータブルＰＣ３５０に利用機器を選択的に変更する場合の手順を図８のフローチャートに基づいて説明する。この実施形態を適用する携帯電話機１００は、キー操作部１２１に機器交換ボタンを備えている。ポータブルＰＣ３５０は図２のブロック図を用いて説明した携帯電話機と同様の通信機能を有する以外は、一般的なコンピュータであるので詳細な説明は省略する。す

なわち、キーボード、およびディスプレイ、ＲＳ２３２Ｃの通信ポート（図２の通信インターフェース１１１に相当）を外部に備え、内部にＣＰＵ（図２の制御部１０９に相当）、メイン・メモリ（図２のＲＡＭ１１５に相当）、ＨＤＤ（図２のＲＯＭ１１３に相当）、フラッシュ・メモリ（図２の不揮発性メモリ１１７に相当）およびＦＤＤなどを収納している。ＣＰＵで処理したデータはＨＤＤに保存されるとともに、通信ポートを経由して外部に転送でき、また外部から受け取ってＣＰＵまたはフラッシュ・メモリに格納することもできる。

【００４１】

最初に携帯電話機のＲＳ２３２Ｃ通信インターフェースとポータブルＰＣのＲＳ２３２Ｃ通信ポートをシリアル・ケーブル３５１で接続する。ブロック３６１では、携帯電話機の機器交換ボタンを操作する。ブロック３６３では不揮発性メモリ１１７に格納されていた識別番号、電話番号およびパスワードなどの機器を変更するためのデータをケーブル３５１を経由してポータブルＰＣ３５０のフラッシュ・メモリに転送し、同時に携帯電話機１００の不揮発性メモリ１１７に格納されていたこれらの情報を消去する。ここで、機器変更データの転送は、通信ポートを利用しないで、不揮発性の記録媒体を経由して行ってもよい。識別番号などを失った携帯電話機１００は以後使用できない状態になる（ブロック３６５）。

【００４２】

一方ポータブルＰＣ３５０はブロック３６７で機器変更データを受け取り、ブロック３６９でポータブルＰＣ内のフラッシュ・メモリに格納する。その後ブロック３７１でポータブルＰＣの通信機能が使用できる状態になる。この状態でポータブルＰＣは図５で説明した手順にしたがって基地局と通信し通信の終了時にはパスワードを変更する。この実施形態では、携帯電話機１００の機器変更データが盗用されて他の通信端末装置に転送されても、ポータブルＰＣ３５０で通信を行おうとした場合に、盗用者の利用によりパスワードが変更されているので不正使用の通知を受け取り、正規の契約者はコピー端末の出現に気付く。盗用者が通話または通信終了時にパスワードを変更しない操作を行ったとしても、前述のとおり通信事業者により同一パスワードの利用により通信停止の処置がとられる

か、その後の正規の利用者の通信でパスワードが変更され、それ以上の不正使用はできない。

【００４３】

このように一契約で複数の通信端末装置を利用させることにより、国間で携帯電話の周波数が異なる場合などに、機器変更データを転送し一契約のもとで複数の周波数の携帯電話機を利用できるようにすることができる。以上の発明の実施の形態は例示として説明したものであり限定的に解釈されるべきではなく、本発明の範囲はあくまで特許請求の範囲に記載された範囲において解釈されるべきである。

【００４４】

【発明の効果】

本発明により、識別情報およびパスワードを格納した不揮発性メモリを備える通信端末装置から前記識別情報および前記パスワードを格納した記憶装置を備えるネットワークに通信する際に、パスワードが盗用され他の通信端末装置に設定されコピー端末として使用されたときに、正規の契約者がその状態を容易に認識できる通信方法および通信端末装置を提供することができた。さらに一契約のもとでユーザに複数の通信端末装置を選択的に利用させても、不正にコピー端末が製作され使用されることを容易に発見して防止できる通信方法および通信端末装置を提供することができた。

【図面の簡単な説明】

【図１】本発明の実施形態を説明するための携帯電話ネットワークの概略図である。

【図２】本発明の実施の形態としての携帯電話機の概略ブロック図である。

【図３】ＲＯＭ１１３の構成を示す図である。

【図４】不揮発性メモリ１１７の構成を示す図である。

【図５】本発明の実施形態を説明するためのフローチャートである。

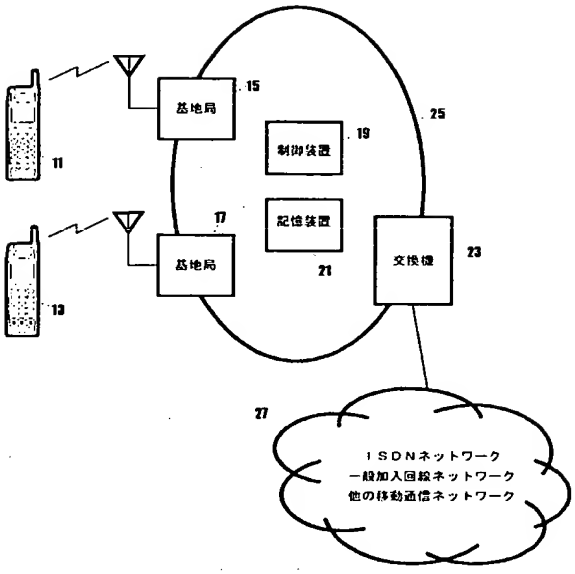
【図６】契約者情報テーブルの実施形態を示す図である。

【図７】本発明の他の実施形態を示す図である。

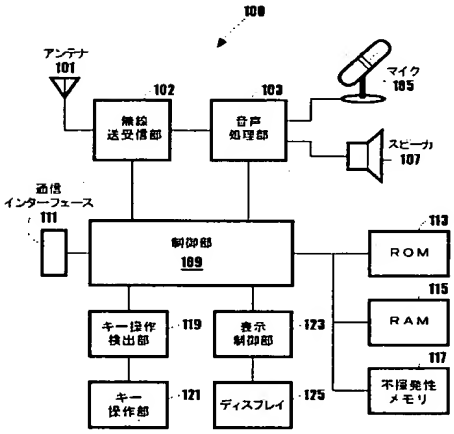
【図８】本発明の他の実施形態を示すフローチャートである。

【書類名】　　図面

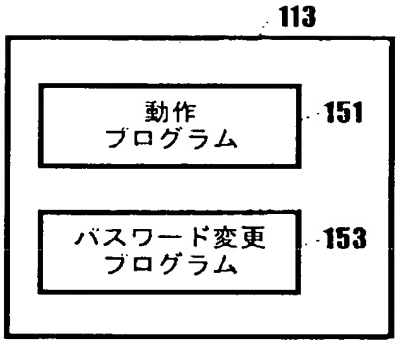
【図１】


基地局
15
11
制御装置
19
25
記憶装置
17
基地局
21
交換機
23
13
27
ＩＳＤＮネットワーク
一般加入回線ネットワーク
他の移動通信ネットワーク

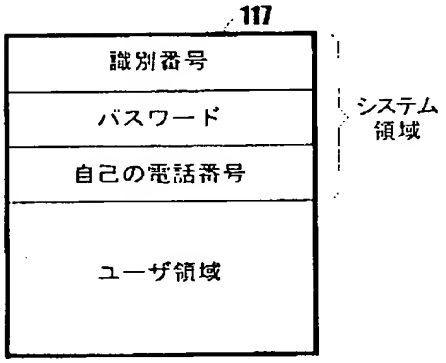
【図２】


100
アンテナ
101
マイク
105
102
103
無線
送受信部
音声
処理部
スピーカ
107
通信
インターフェース
111
113
制御部
109
ROM
115
RAM
キー操作
検出部
119
表示
制御部
123
117
不揮発性
メモリ
キー
操作部
121
ディスプレイ
125

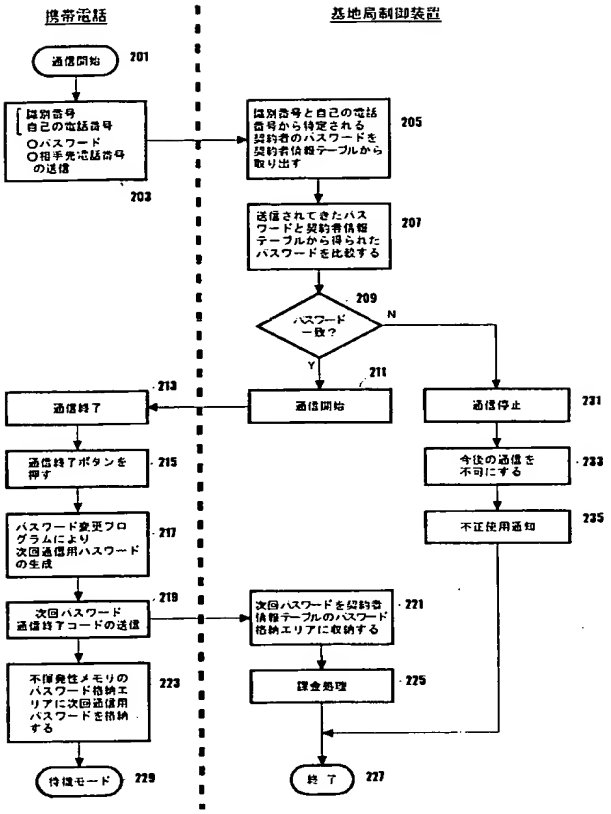
【図３】


113
動作
プログラム
151
パスワード変更
プログラム
153

【図４】


117
識別番号
パスワード
自己の電話番号
ユーザ領域
システム
領域

【図５】

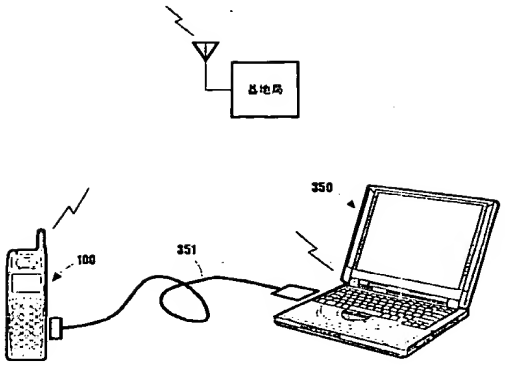


【図６】

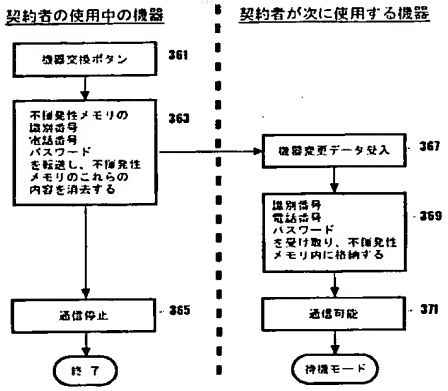
契約者	契約番号	電話番号	パスワード	課金情報	住所	・・・
A	AA	AA-AAAA	A001			・・・
B	BB	BB-BBBB	B001			・・・
C	CC	CC-CCCC	C001			・・・
⋮	⋮	⋮	⋮	⋮	⋮	⋮

契約者情報テーブルの例
300

【図７】


基地局
350
351
100

【図８】


契約者の使用中の機器
契約者が次に使用する機器
機器交換ボタン
361
不揮発性メモリの
識別番号
電話番号
パスワード
を転送し、不揮発性
メモリのこれらの
内容を消去する
363
機器変更データ受入
367
識別番号
電話番号
パスワード
を受け取り、不揮発性
メモリ内に格納する
369
通信停止
365
通信可能
371
終了
待機モード

【書類名】　要約書

【要約】

【課題】識別情報およびパスワードの識別結果によりネットワークへの通信が許可される携帯電話機においてパスワードを盗用したコピー電話機の不正な使用をを防止する。

【解決手段】本発明の通信方法は、（ａ）通信の開始時に携帯電話機の不揮発性メモリに格納した識別情報およびパスワードをネットワークに送信するステップと、ステップ（ａ）で送信したパスワードとは異なるパスワードを通信が終了する前に生成するステップと、（ｃ）生成したパスワードを携帯電話機の不揮発性メモリに格納するステップと、（ｄ）生成したパスワードを前記ステップ（ａ）で開始した通信が終了する前にネットワークに送信するステップとを有する。通信のたびにパスワードが自動的に更新されているので、コピー電話機の利用が防止できる。

【選択図】図１

認定・付加情報

特許出願の番号	特願２０００－０９８８１８
受付番号	５００００４１０１２７
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　４月　３日

＜認定情報・付加情報＞

【提出日】　平成12年 3月31日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　１９９０年１０月２４日
［変更理由］　新規登録
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレイション

２．変更年月日　　２０００年　５月１６日
［変更理由］　名称変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション